EXHIBIT B

Wireless Engineering Audit:

Enterprise Wireless Network

Logan International Airport

Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909

Prepared By: Jason McClafferty
Prep Reference No.: V1.02
Date: 16-September-05

This Page was intentionally left blank

Table of Contents

RF Vendor Contacts

BeyondWire Technologies
Corporate Offices:
360 South Jefferson Street
Kittanning, PA 16201
Phone: 724-545-1115 Fax: 724-545-7815

The representatives responsible for the contents of this document are:

Field Engineers:
Jason McClafferty
BeyondWire Technologies 724-545-1115 x 223

Project Manager
F. Brent Hester 725-545-1115 x 222

Massachusetts Port Authority and Advanced Wireless Group, LLC representatives supplying information used in this document are:

David Ziembicki
Jeffrey Ziembicki
Deborah Kee

I hereby declare under penalty of perjury that this Wireless Engineering Audit was prepared by me, or under my direction, and that the facts recited herein are true and correct, as found in the Engineering audit conducted September 12 though 15, 2005.

Jason McClafferty
Jason McClafferty

Date: 09-27-2005

OVERVIEW

On September 12 - 15, 2005, a site engineering audit was conducted for the Logan International Airport located in Boston, MA. This audit was conducted to determine the coverage patterns of the existing Central WIFI Antenna System and areas of potential interference that would compromise the networks quality. This audit was conducted in specific areas designated by the IT Department of Advanced Wireless Group, LLC and Massachusetts Port Authority.

This report is based upon the specific findings of the site survey. Including the requirements as conveyed at the time of the site survey, as well as coverage provided in the Scope of Work Document.

All findings will apply to the Logan International Airport site coverage unless:

- Massachusetts Port Authority: Physically changes or remodels any of the facility with new or rearranged structural items.
- Massachusetts Port Authority: Changes the location or positioning of an Access Point Radio, which can affect RF propagation.
- Massachusetts Port Authority: Installs additional equipment emitting electromagnetic radiation fields and affecting RF propagation.

This audit contains information pertaining to 2.4 GHz unlicensed band, more specifically, Cisco Systems Wireless Networking Solutions product utilized in the Central WIFI Antenna System within Logan International Airport.

This Page was intentionally left blank

Specific Audit Locations

Identifying Information:

- Terminal B Pier B Level 1 – Baggage Claim
- Terminal B Pier B Level 2 – Ticketing
- Terminal C Level 1 Pier D – Baggage Claim
- Terminal C Level 2 Pier D – Gates 40, 41, 42

This Page was intentionally left blank

Scope of Project:

The audit consists of three primary objectives:

1. To provide a working coverage pattern for the Central WIFI Antenna System in the specified areas throughout the named facilities.

2. To isolate areas of interference that may compromise the Wireless LAN. Identify the cause for interference and map the interference coverage patterns.

3. To isolate areas where the Wireless LAN could interfere with the existing environment.

This Page was intentionally left blank

WLAN Expectations:

- The original design expressed the need to have 100% 802.11b/g coverage throughout the specified areas within the named facilities. TSA Security areas of each facility are specified as key areas in which interference levels are minimal. As well the client wants TSA to have the ability to roam within the coverage patterns of each building.

- The original design requires an IEEE 802.11b/g coverage pattern of 54 Mbps in the heavily used areas of the facilities. The radio settings will allow association at 5.5Mbps.

- The original design requires a seamless wireless system based on industry standards that apply to the equipment utilized in this project.

This Page was intentionally left blank

Customer Provided Information:

The original wireless network design consists of only TCP/IP traffic protocol.

Massachusetts Port Authority connected the wireless segment(s) on separate VLANs, and receives no broadcast from other segments. VLANs are divided into management, public safety, tenant, and WIFI. The client has expressed the critical need and ability to control the VLANs and deactivate all connections except for public safety in the event of an emergency.

In the original design, services supplied to the wireless client were determined to be above basic service. (File transfer, Internet traffic, and HTML based applications were included) There was no throughput information provided for design but considerations to dedicate all bandwidth to the public safety VLAN in the event of an emergency is critical.

This Page was intentionally left blank

Executive Summary

On the week of September 12, 2005 a planned audit was conducted within the Terminal C Pier D and Terminal B Pier B areas of Logan International Airport. The objective of this audit is to identify areas of interference, determine the source for the interference, map the interfering coverage pattern and document the performance impact of the public safety network within these areas.

As explained to BeyondWire Technologies: Massachusetts Port Authority's original design criteria for the Central WIFI Antenna System requires the ability to control access to the wireless network by disabling any non Public Safety wireless device connected to the network or within the RF coverage patterns while providing seamless roaming within and between critical areas. The design is to provide Public Safety users with optimal coverage and the all bandwidth within the 802.11b/g spectrum in the event of and emergency.

At the time of the audit BeyondWire Technologies did locate interfering and competing frequency devices with in critical areas of Public Safety.

Using the design criteria provided by Massachusetts Port Authority and information collected from an AirMagnet Laptop Analyzer, Anritsu Spectrum Analyzer and Helium Network's Wireless Recon device, measurements for interference and the areas affected by the interference were mapped and documented. Please reference the Summary by Location portion and the Concerns portion of this report.

This Page was intentionally left blank

Wireless Audit Equipment

802.11b/g Wireless Audit Equipment

The following equipment was used in Massachusetts Port Authority's Logan International Airport's site audit.

Spectrum Analyzer

Anritsu MS2711A handheld spectrum analyzer, 10 MHz – 3.0 GHz
Firmware Version: 1.35, 2.0dBi gain dipole antenna system

RF Network Management tools

AirMagnet Laptop Analyzer Version 5.0 (Build 3611)

Helium Networks, Inc. Wireless Recon
SiteScout and SiteSense v1.0

Portable Computer Systems

IBM ThinkPad T42 Portable Laptop Computer System
Intel Centrino, 1.5 GHz, 256meg ram, Windows XP

Hewlett Packard Omni Book 6000 Portable Laptop Computer System
PIII, 900 MHz, 256meg ram, Windows 2000

Client Adapter

Cisco AIR-CB21AG-A-K9
Available Power Settings 802.11b/g -

- 20 dBm (100 mW) @ 1, 2, 5.5 and 11 Mbps
- 18 dBm (63 mW) @ 1, 2, 5.5, 6, 9, 11, 12, 18 and 24 Mbps
- 17 dBm (50 mW) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24 and 36 Mbps
- 15 dBm (30 mW) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36 and 48 Mbps
- 13 dBm (20 mW) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54 Mbps
- 10 dBm (10 mW) @ 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54 Mbps

Antenna System - Integrated diversity dual-band 2.4/5 GHz antenna
Receiver Sensitivity - -94 dBm @ 1 Mbps

Software / Firmware Version - 1.0.0.322

Summary Test Procedure

Short summary of site definition and performance:

Wireless LAN testing is summarized by using a matrix consisting of density, desired throughput, terrestrial/structural challenges, and performance.

All engineering and samples were conducted using passive and active tests. Passive testing provides radio capabilities in native format. The active tests duplicates passive testing with the exception of using radio plus data packets.

We used a -70 DBm guideline for tests to determine the distance of coverage in most environments.

Rogue AP detection and interference identification was conducted by walking the coverage pattern on separate occasions while using AirMagnet Laptop Analyzer and Anristu Spectrum Analyzer.

RF coverage mapping of the Central WIFI Antenna System and identified rogue access points was conducted by walking the identified areas with Helium Networks Wireless Recon device.

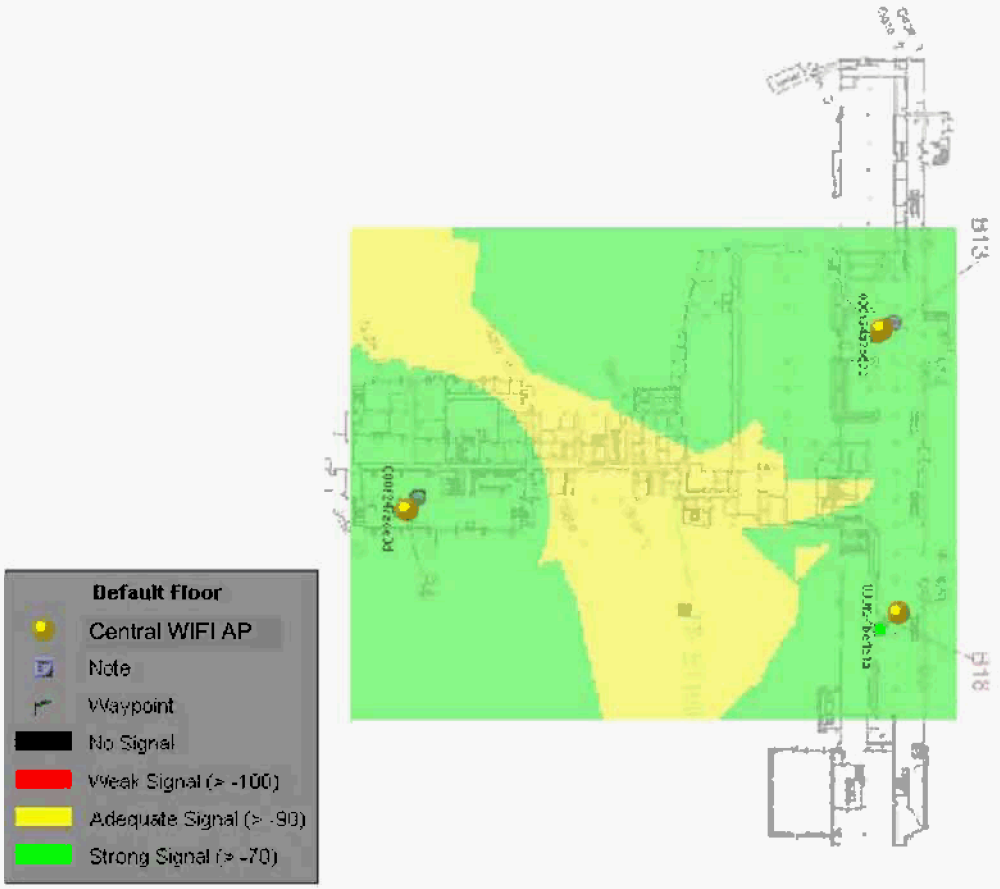
This Page was intentionally left blank

Summary by Location

Terminal B Pier B Level 1

Central WIFI Antenna System coverage pattern

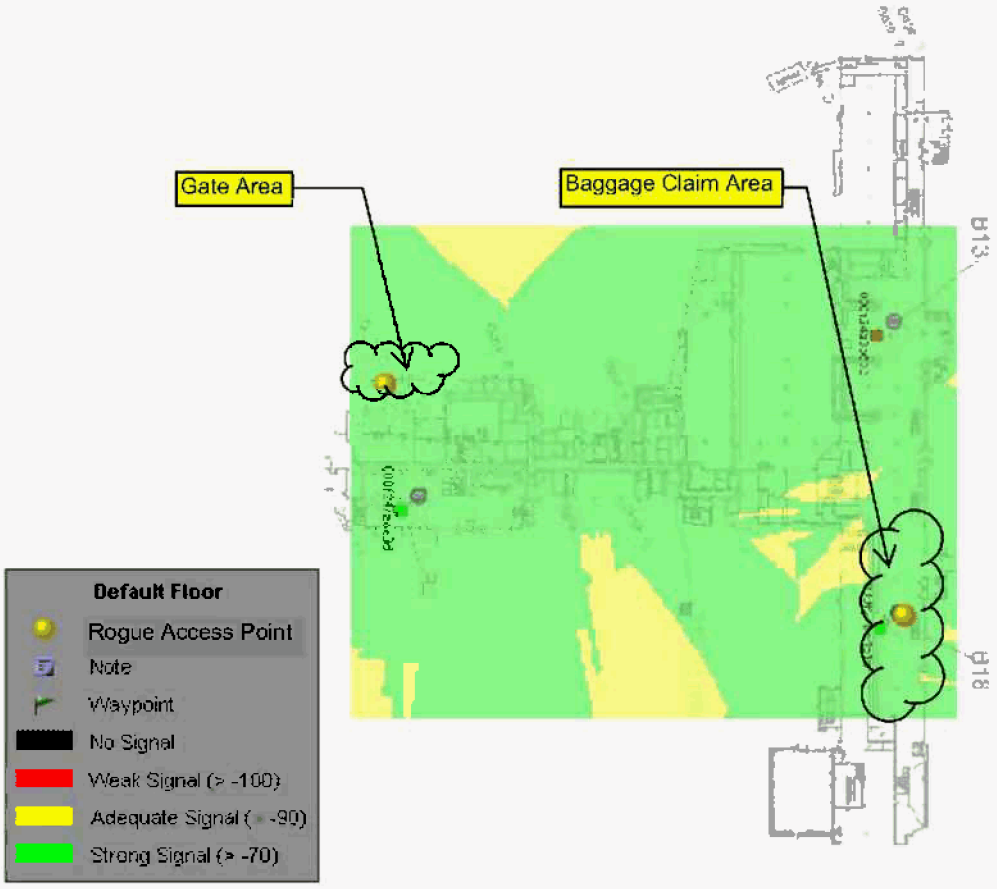
This image indicates the coverage pattern for the Central WIFI Antenna System. The access points that provide coverage to this area are displayed on the map.



Competing Frequencies

Terminal B Pier B Level 1

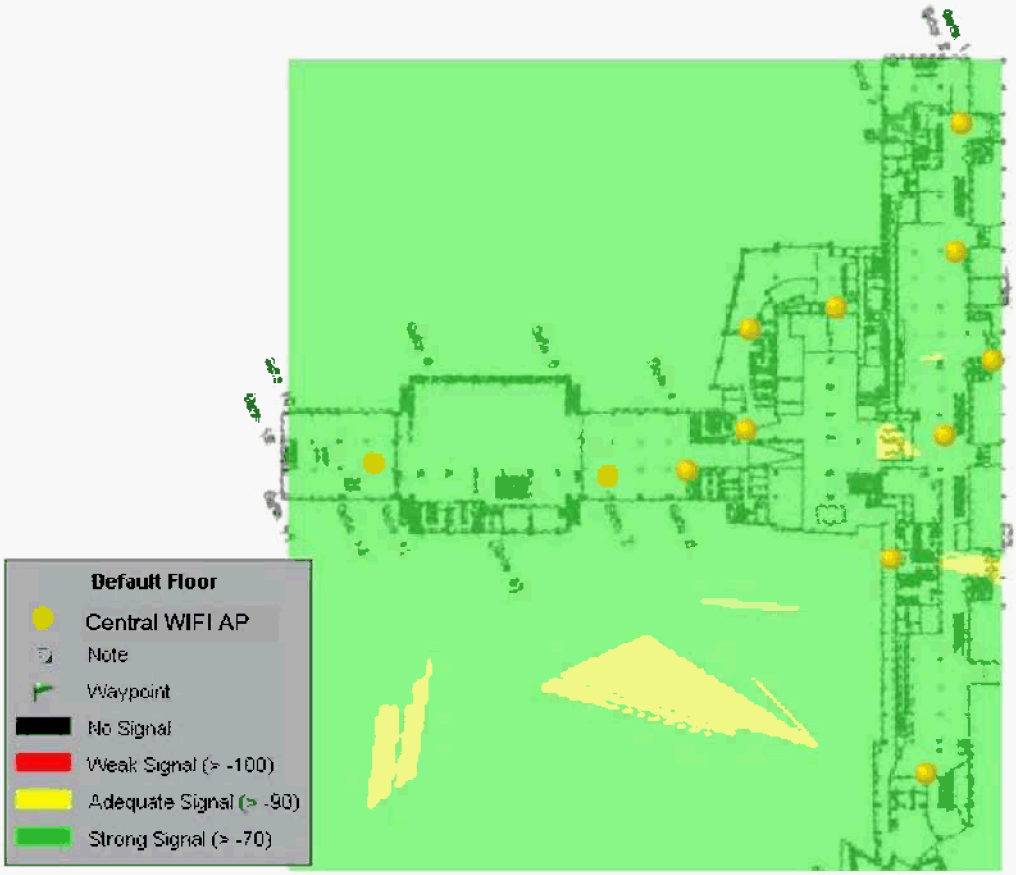
In RF sweeps of the facility, RF findings indicated interference from rogue access points located in the Gate and Baggage Claim areas. The following image is the coverage pattern of the rogue access points. The coverage pattern of the rogue access points and the coverage pattern of Central WIFI Antenna System are in direct competition for the bandwidth in this area.



Terminal B Pier B Level 2

Central WIFI Antenna System coverage pattern

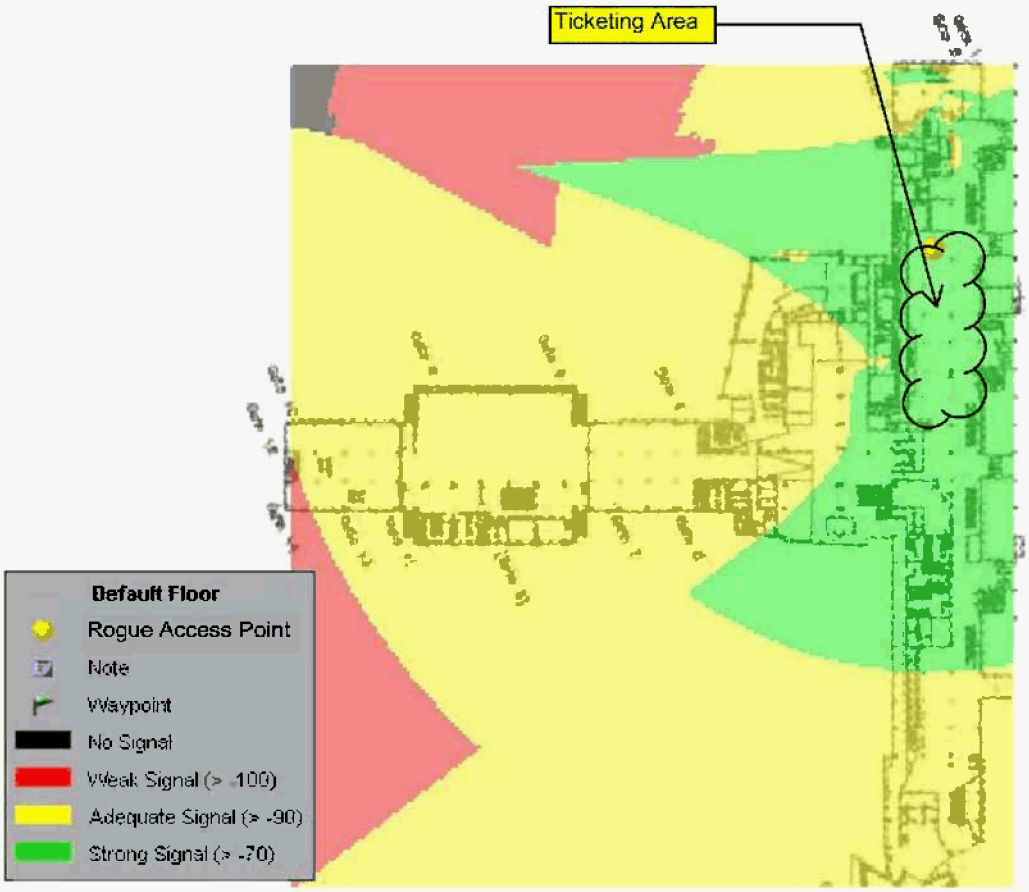
This image indicates the coverage pattern for the Central WIFI Antenna System. The access points that provide coverage to this area are displayed on the map.



Competing Frequencies

Terminal B Pier B Level 2

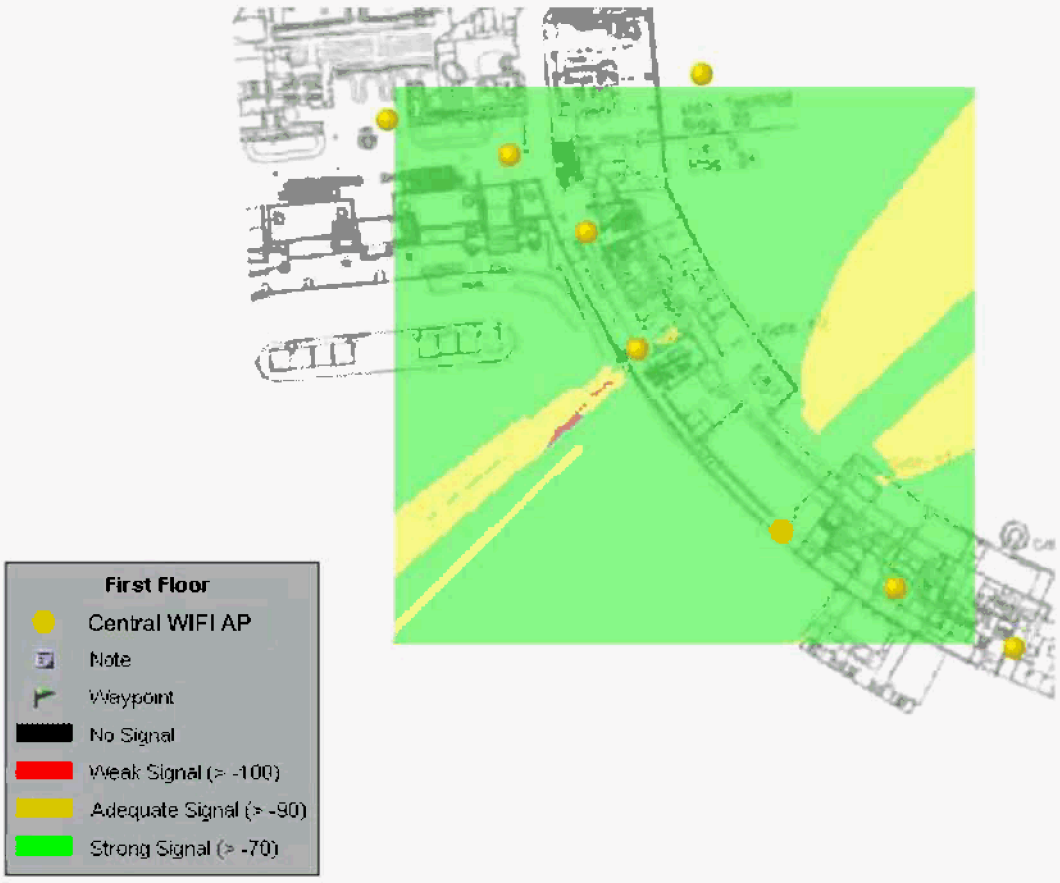
In RF sweeps of the facility, RF findings indicated interference from a rogue access point located in the ticketing area. The following image is the coverage pattern of that rogue access point. The coverage pattern of the rogue access point and the coverage pattern of Central WIFI Antenna System are in direct competition for the bandwidth in this area.



Terminal C Pier D Level 1

Central WIFI Antenna System coverage pattern

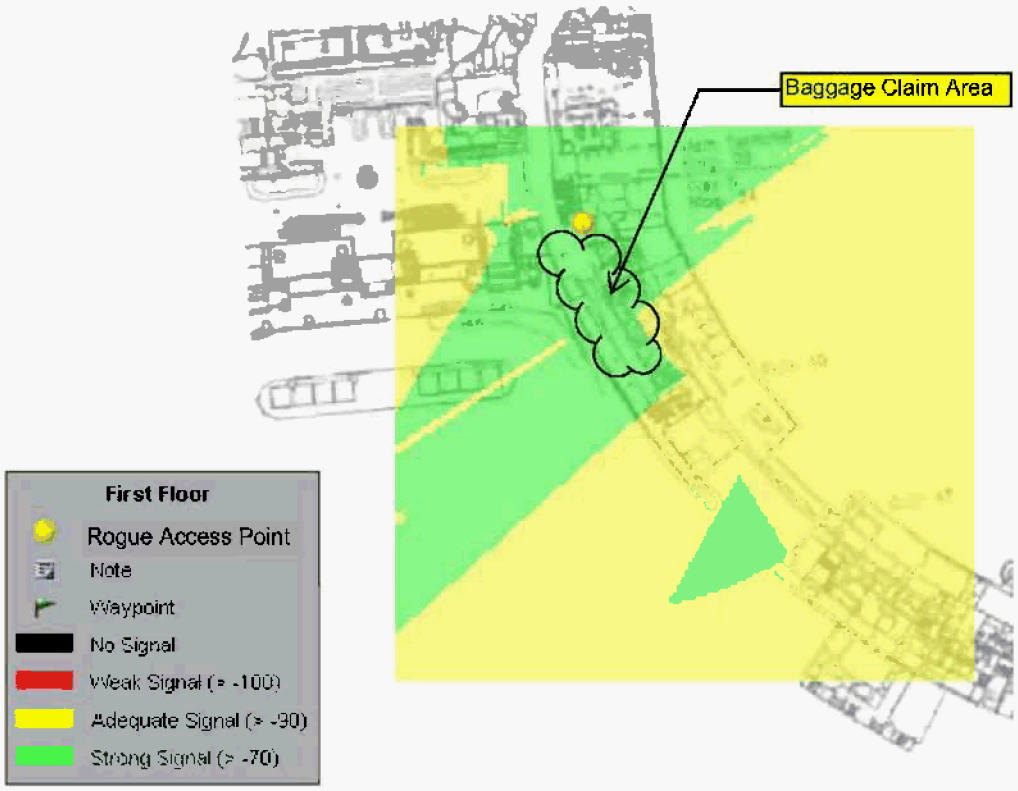
This image indicates the coverage pattern for the Central WIFI Antenna System. The access points that provide coverage to this area are displayed on the map.



Competing Frequencies

Terminal C Pier D Level 1

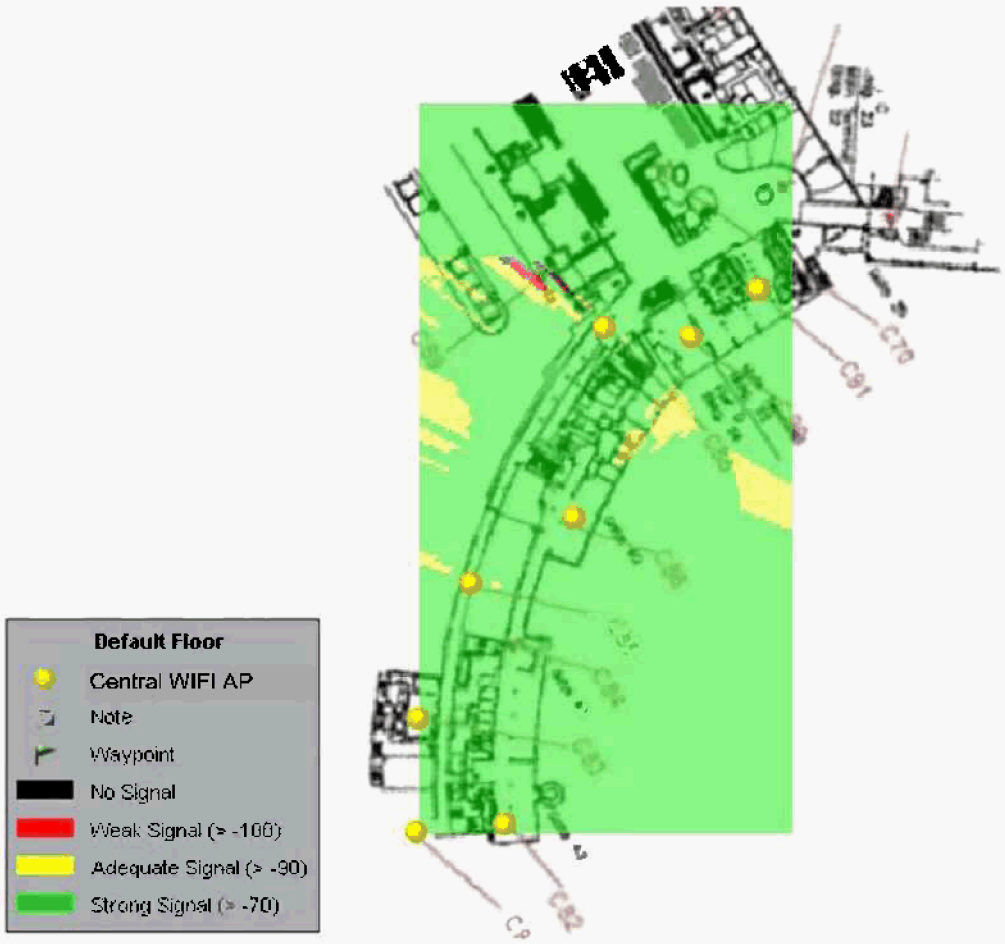
In RF sweeps of the facility, RF findings indicated interference from a rogue access point located in the Baggage Claim area. The following image is the coverage pattern of that rogue access point. The coverage pattern of the rogue access point and the coverage pattern of Central WIFI Antenna System are in direct competition for the bandwidth in this area.



Terminal C Pier D Level 2

Central WIFI Antenna System coverage pattern

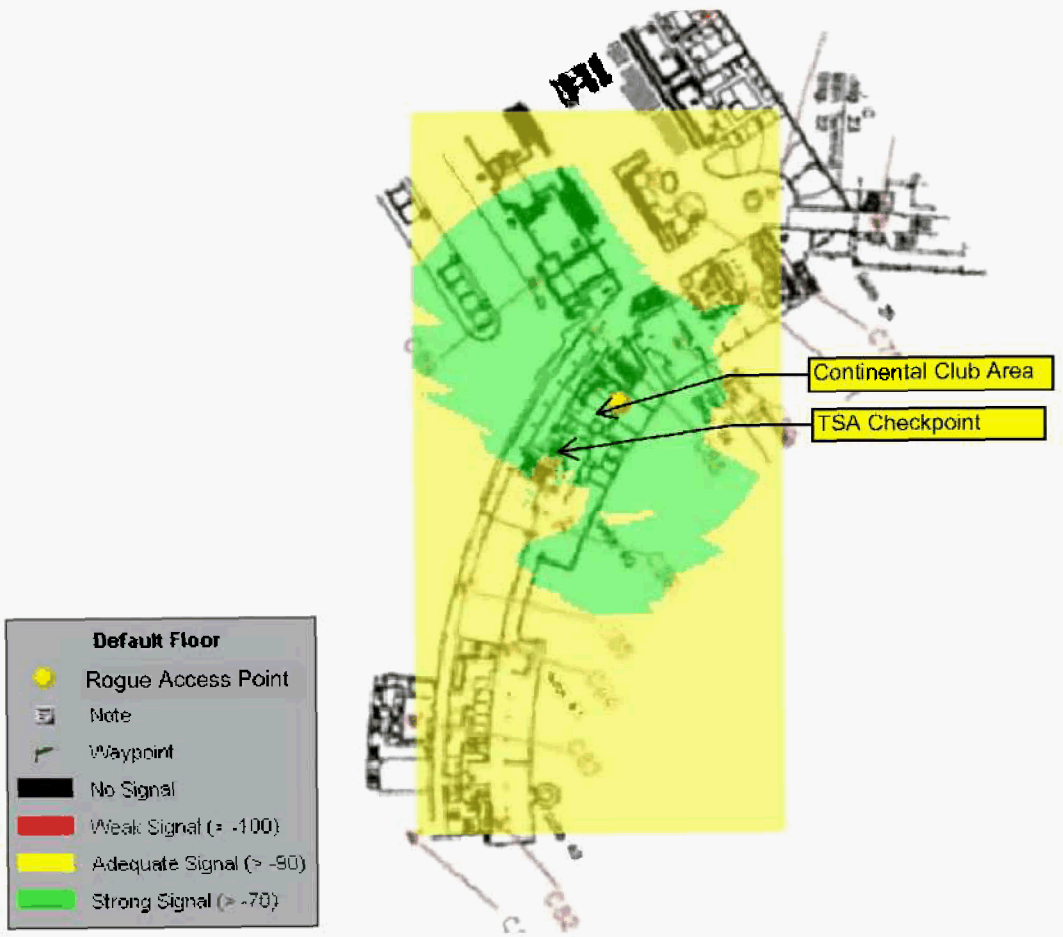
This image indicates the coverage pattern for the Central WIFI Antenna System. The access points that provide coverage to this area are displayed on the map.



Competing Frequencies

Terminal C Pier D Level 2

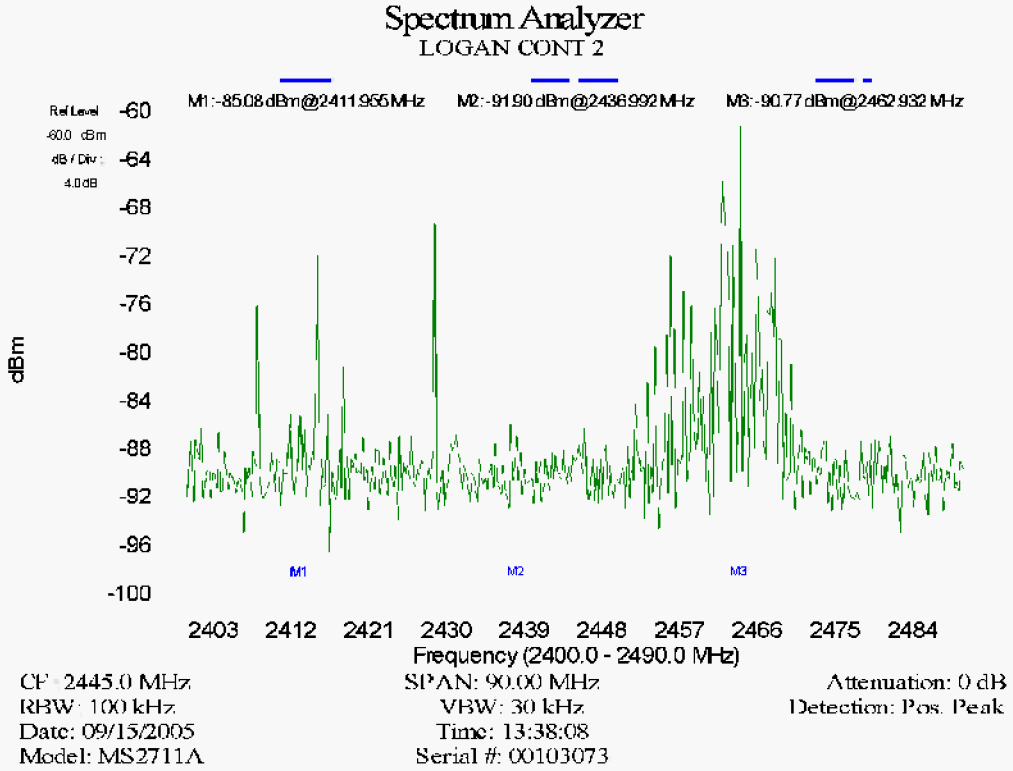
In RF sweeps of the facility, RF findings indicated interference from a rogue access point located in the Continental Club area. The following image is the coverage pattern of that rogue access point. The coverage pattern of the rogue access point and the coverage pattern of Central WIFI Antenna System are in direct competition for the bandwidth in this area.



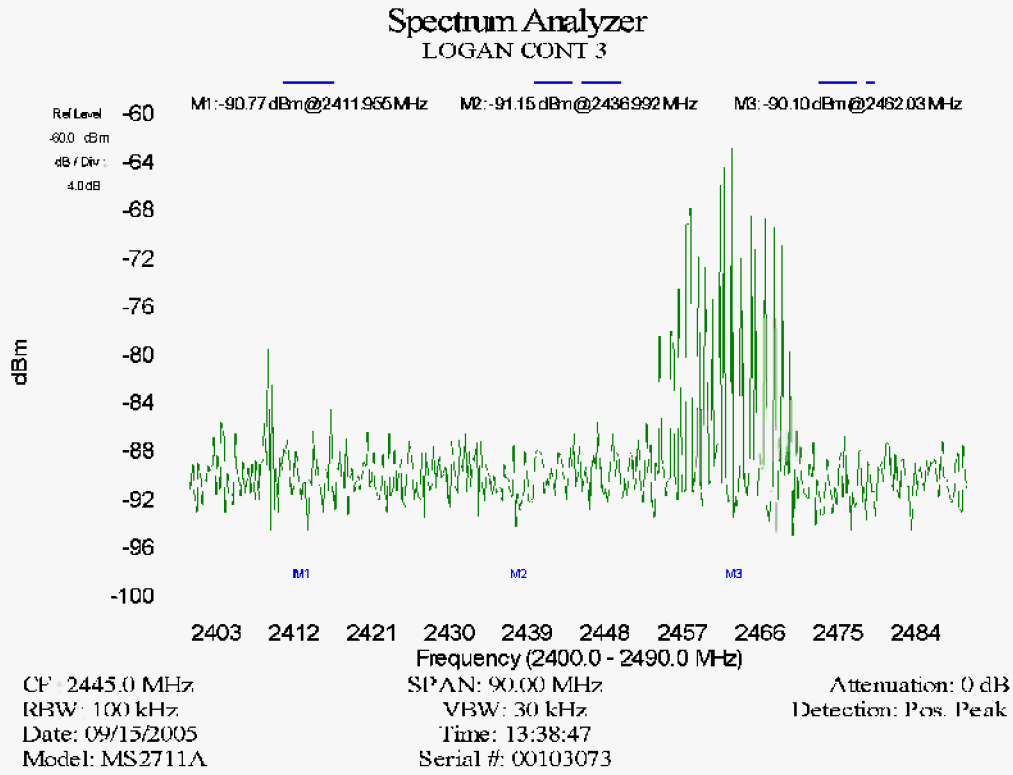
Spectrum Analysis

Terminal C Pier D Level 2

The following image of the 802.11b/g spectrum is of data collected with the Anritsu Spectrum Analyzer near the TSA Checkpoint in Pier D. Each blue marker represents the center band channels. This checkpoint has a microcell coverage pattern from the Central WIFI Antenna System utilizing the three center band channels for the 802.11b/g spectrum.



The following image of the 802.11b/g spectrum is of data collected with the Anritsu Spectrum Analyzer near the Continental Club in Pier D adjacent to the TSA Checkpoint noted above. Each blue marker represents the center band channels. The rouge coverage pattern is utilizing channel 11 as indicated in graph below.



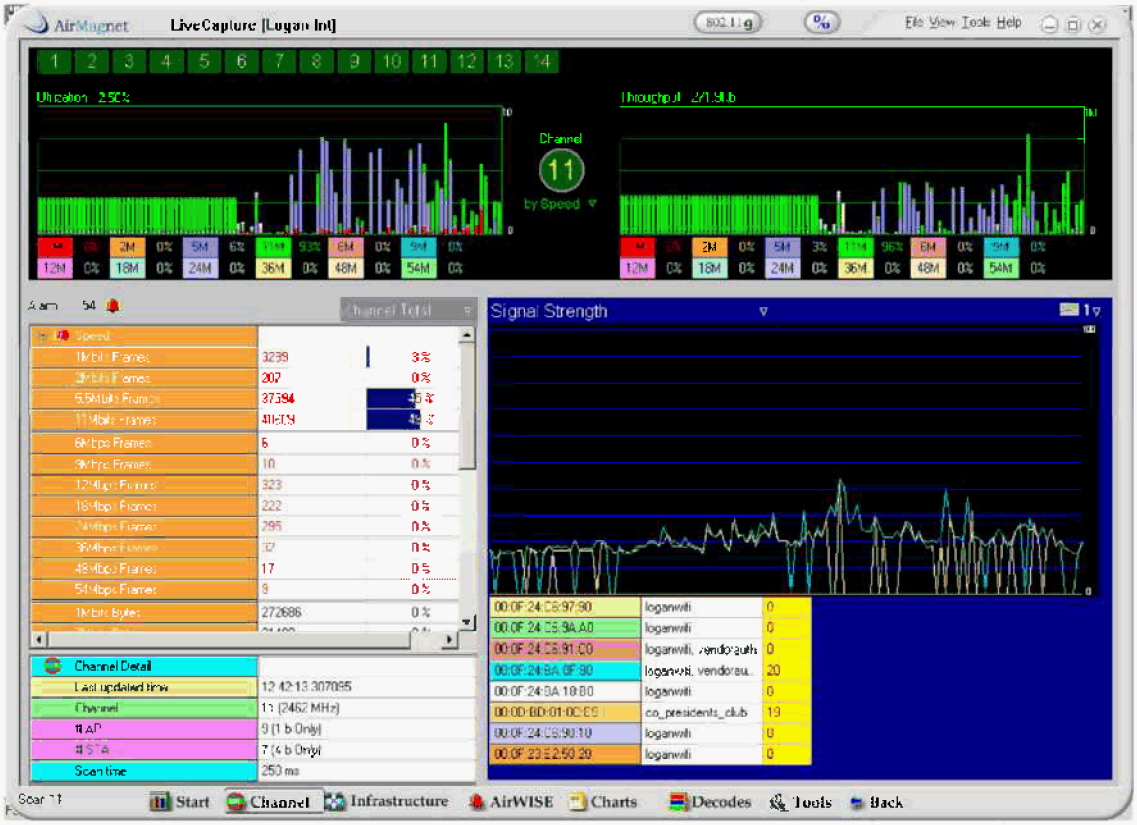
Concerns

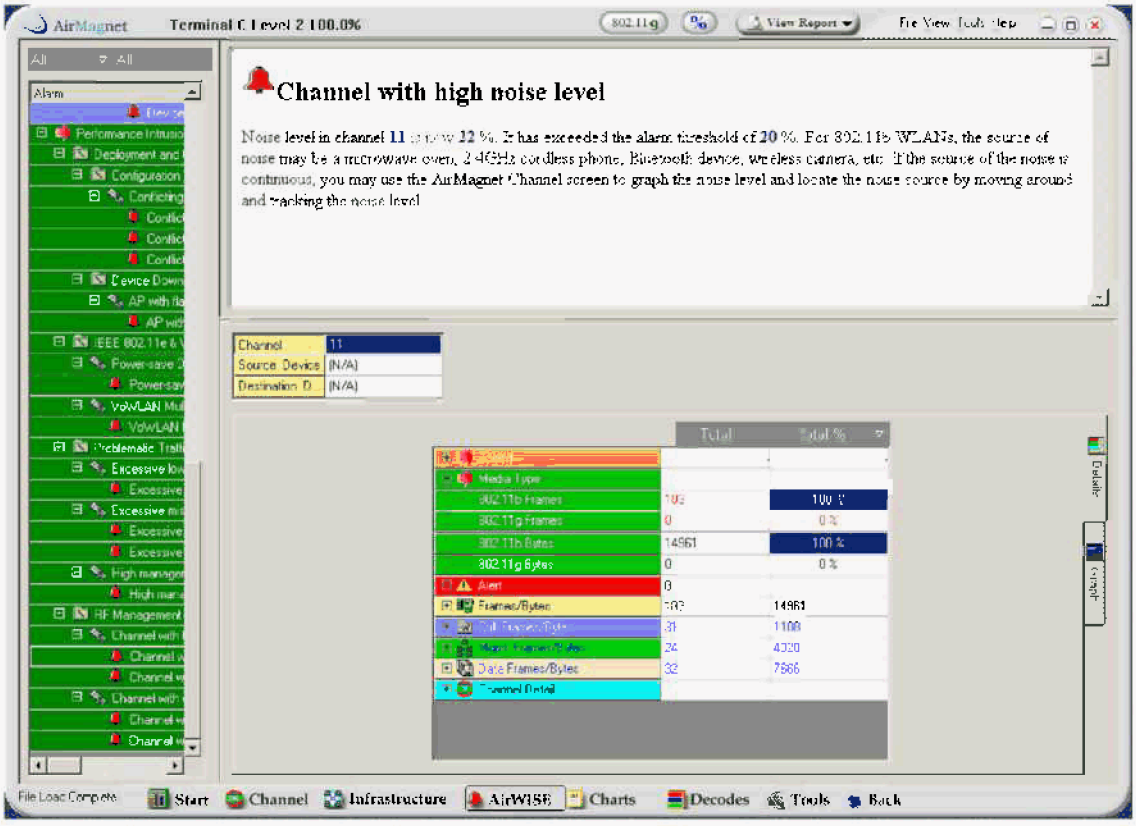
Logan International Airport

The original microcell/picocell design required overlapping coverage in key areas of the facility. The microcell/picocell design provides redundant coverage to high usage areas and key areas of public safety. This design does not support the stacking of access points in these areas. Wireless signals of adequate strength were detected from rogue access points within these key areas. The presence of these access points can degrade the capacity of the Central WIFI Antenna System and there is some unavoidable channel overlap between the Central WIFI Antenna Systems and these AP's.

There are a number microwaves within the club areas and lunch rooms which could impact the 802.11b/g wireless signal and might degrade the packet transmission from time to time when the microwaves are in use. Also, the conveyor belts are powered by heavy duty electronic motors and EMF forces from the conveyors negatively impact the radio signals especially every time they start and stop. But since this interference is only of short duration and happens very infrequently the chances of it having a major negative impact on the operation of WLAN are small.

The following images are screen captures from the AirMagnet for channel 11. The readings are from a location outside the TSA checkpoint in Terminal C Pier D Level 2. AirMagnet AirWISE reported a high noise level on channel 11 in this area.




AirMagnet
Terminal C Level 2 100.0%
802.11g
View Report
Channel with high noise level
Noise level in channel 11 is now 22 %. It has exceeded the alarm threshold of 20 %. For 802.11b WLANs, the source of noise may be a microwave oven, 2.4GHz cordless phone, Bluetooth device, wireless camera, etc. If the source of the noise is continuous, you may use the AirMagnet Channel screen to graph the noise level and locate the noise source by moving around and tracking the noise level
Channel 11
Source Device (N/A)
Destination D (N/A)
Total
Total %
Media Type
802.11b Frames
802.11g Frames
802.11b Bytes
802.11g Bytes
Alert
Frames/Bytes
Data Frames/Bytes
Start
Channel
Infrastructure
AirWISE
Charts
Decodes
Tools
Back

This Page was intentionally left blank

Rogue Access Points

Rogue Access Point List – December 2003

Location	SSID	AP Name or MAC Address
Terminal B:		
American West Bagage Check	cheers	AP350-56948c
American West Curbside Bagage Check	"not broadcast"	Aronet:b9:50:3a
American Curbside Bagage Check	flytrap	Aronet40:14:30
American Bagage Check	flytrap	AABOSAP01-WAP02
American Club	tmobile	10.240.40.3
American Club	tmobile	00:0b:be:ea:9d:c2
ATA Ticketing	"not broadcast"	Aironet40:22:2c
Terminal C:		
Contenetal Baggage Claim	fsbaguser	BOSA350_C01A
	9klogan	Microsoft:CA.E5:3E

Newly discovered rogue access point list – April 2005

Note: The rogue access points without an SSID were present but were not broadcasting the SSID or did not have a client associated at the time of discovery.

Location	SSID	AP Name or MAC Address
Terminal B:		
US Air – Main Terminal	CHEERS	BOSTKTWIRELESS
US Air – Main Terminal	(non-broadcast)	BOSWIRELESS BSO
		AIRONET :40:14:30
US Air – Main Pier – Gate 8		BOSR-GATE8-AP01
US Air – Main Pier – Gate 9		BOSR-GATE9-AP01
US Air – Gates 15-21		00:0d:28:88:c8:dd
AA – ATO area		Aironet 40:74 21
AA – Main Pier		Aironet :40:14:30
AA – Main Pier		Aironet :40:22:2c
Terminal C:		
Continental President's Club	co_presidents_club	00:0d:bd:01:0c:e9
Continental Ticket Counter	cowlan	BOSA350_C01A
Airport Wireless Store		Linksys Router
United Pier, Near Info Booth, Past CP		Globalsun:2a:02:96

Appendix A – Site Engineering Disclosure

The findings of this survey are primarily for design and implementation of a wireless LAN or bridging system or both. It is understood that any specific details provided pertain to the specific day the sites were surveyed. While this is an indication of what is found on this location on a constant basis, it is not a guarantee or certification that other environmental issues may not exist in this location.

Environments such as these are understood to be changing and may change without warning or notice.

It is also understood that the equipment being surveyed utilizes public RF channels as assigned by the FCC and that all the benefits and complications that come with this are fully understood.

It is understood that the surveyor nor his employer or his company make any warranties, guarantees, or certification expressed or implied, to the information disclosed in this document.

This Page was intentionally left blank

Appendix B - Glossary

Glossary of terms

802.11 Standard

802.11, or IEEE 802.11, is a type of radio technology used for wireless local area networks (WLANs). It is a standard that has been developed by the IEEE (Institute of Electrical and Electronic Engineers), http://standards.ieee.org. The IEEE is an international organization that develops standards for hundreds of electronic and electrical technologies. The organization uses a series of numbers, like the Dewey Decimal system in libraries, to differentiate between the various technology families.

The 802 subgroup (of the IEEE) develops standards for local and wide area networks with the 802.11 section reviewing and creating standards for wireless local area networks.

Wi-Fi , 802.11, is composed of several standards operating in different radio frequencies: 802.11b is a standard for wireless LANs operating in the 2.4 GHz spectrum with a bandwidth of 11 Mbps; 802.11a is a different standard for wireless LANs, and pertains to systems operating in the 5 GHz frequency range with a bandwidth of 54 Mbps. Another standard, 802.11g, is for WLANS operating in the 2.4 GHz frequency but with a bandwidth of 54 Mbps.

802.11a

An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.725 GHz to 5.850 GHz) with a maximum 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz frequency, because the 802.11a specification offers more radio channels than the 802.11b. These additional channels can help avoid radio and microwave interference.

802.11b
International standard for wireless networking that operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835 GHz) and provides a throughput of up to 11 Mbps. This is a very commonly used frequency. Microwave ovens, cordless phones, medical and scientific equipment, as well as Bluetooth devices, all work within the 2.4 GHz frequency band.

802.11g
Similar to 802.11b, but this standard provides a throughput of up to 54 Mbps. It also operates in the 2.4 GHz frequency band but uses a different radio technology in order to boost overall bandwidth.

Access point
A wireless LAN transceiver or "base station" that can connect a wired LAN to one or many wireless devices. Access points can also bridge to each other.

There are various types of access points and base stations used in both wireless and wired networks. These include bridges, hubs, switches, routers and gateways. The differences between them are not always precise, because certain capabilities associated with one can also be added to another. For example, a router can do bridging, and a hub may also be a switch. But they are all involved in making sure data is transferred from one location to another.

A bridge connects devices that all use the same kind of protocol. A router can connect networks that use differing protocols. It also reads the addresses included in the packets and routes them to the appropriate computer station, working with any other routers in the network to choose the best path to send the packets on. A wireless hub or access point adds a few capabilities such as roaming and provides a network connection to a variety of clients, but it does not allocate bandwidth. A switch is a hub that has extra intelligence: It can read the address of a packet and send it to the appropriate computer station. A wireless gateway is an access point that provides additional capabilities such as NAT routing, DHCP, firewalls, security, etc.

Bandwidth
The amount of transmission capacity that is available on a network at any point in time. Available bandwidth depends on several variables such as the rate of data transmission speed between networked devices, network overhead, number of users, and the type of device used to connect PCs to a network. It is similar to a pipeline in that capacity is determined by size: the wider the pipe, the more water can flow through it; the more bandwidth a network provides, the more data can flow through it. Standard 802.11b provides a bandwidth of 11 Mbps; 802.11a and 802.11g provide a bandwidth of 54 Mbps.

HotSpot
A place where you can access Wi-Fi service. This can be for free or for a fee. HotSpots can be inside a coffee shop, airport lounge, train station, convention center, hotel or any other public meeting area. Corporations and campuses are also implementing HotSpots to provide wireless Internet access to their visitors and guests. In some parts of the world, HotSpots are known as Cool Spots.

LAN
A system of connecting PCs and other devices within the same physical proximity for sharing resources such as an Internet connections, printers, files and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN.

MAC
Every wireless 802.11 device has its own specific MAC address hard-coded into it. This unique identifier can be used to provide security for wireless networks. When a network uses a MAC table, only the 802.11 radios that have had their MAC addresses added to that network's MAC table will be able to get onto the network.

PC card
A removable, credit-card-sized memory or I/O device that fits into a Type 2 PCMCIA standard slot, PC Cards are used primarily in PCs, portable computers, PDAs and laptops. PC Card peripherals include Wi-Fi cards, memory cards, modems, NICs, hard drives, etc.

Peer-to-peer network
A wireless or wired computer network that has no server or central hub or router. All the networked PCs are equally able to act as a network server or client, and each client computer can talk to all the other wireless computers without having to go through an access point or hub. However, since there is no central base station to monitor traffic or provide Internet access, the various signals can collide with each other, reducing overall performance.

Range
How far will your wireless network stretch? Most Wi-Fi systems will provide a range of a hundred feet or more. Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to mile.

Site survey
The process whereby a wireless network installer inspects a location prior to putting in a wireless network. Site surveys are used to identify the radio- and client-use properties of a facility so that access points can be optimally placed.

WEP
Basic wireless security provided by Wi-Fi. In some instances, WEP may be all a home or small-business user needs to protect wireless data. WEP is available in 40-bit (also called 64-bit), or in 108-bit (also called 128-bit) encryption modes. As 108-bit encryption provides a longer algorithm that takes longer to decode, it can provide better security than basic 40-bit (64-bit) encryption.

WLAN
Also referred to as LAN. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.

Terminal Building: A building or an area of building that is usually the main entrance to a gate area. They usually house ticketing, baggage checking and pick up.

Interconnect: A connecting hallway between two areas

AP: abbreviation for an Access Point

Directional Antenna: An antenna that concentrates transmission power into a direction increasing coverage distance at the expense of coverage angle. Directional antenna types include Yagi, Patch and Parabolic Dish.

Spread Spectrum: A radio transmission technology that "spreads" the user information over a much wider bandwidth than otherwise required in order to gain the benefits such as improved interference tolerance and unlicensed operation.

Radio Frequency (RF): A generic term for radio-based technology.

Range: A linear measure of the distance that a transmitter can send a signal.

Omni-Directional Antenna: An antenna that provides a 360-degree transmission pattern. These types of antennas are used when coverage in all directions is required.

Gain: A method of increasing the transmission distance of a radio by the concentration of its signal in a single direction, typically through the use of a directional antenna. Gain does not increase radios signal strength, but simply redirects it. Therefore as gain increases, the decrease in angle of coverage is inversely proportional.

Frequency Hopping Spread Spectrum (FHSS): A type of spread spectrum radio transmission in which the transmitter and receiver hop in synchronization from one frequency to another according to a prearranged pattern.

Direct Sequence Spread Spectrum (DSSS): A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

Roaming: A feature of some access points that allow users to move through a facility while maintaining unbroken connection to the LAN

Notes: A comment or an explanation, as on a passage in a text.

Waypoint: A point between major points on a route, as along a track. A point of reference, a location (definition is for the chart legend)